

Entorno personal de aprendizaje:

Curso de Ciberseguridad: Seguridad en medios digitales



Ministerio de
**TECNOLOGÍAS
DE LA INFORMACIÓN
Y COMUNICACIÓN**

 **GOBIERNO
NACIONAL**

*Paraguay
de la gente*

Unidad 3. Ingeniería Social

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Viceministerio de Tecnologías de la Información y Comunicación

Director General de Inclusión Digital y TIC en la Educación

Dirección General de Ciberseguridad y Protección a la Información

SEDE 1



Ministerio de
**TECNOLOGÍAS
DE LA INFORMACIÓN
Y COMUNICACIÓN**

Dirección: Complejo Santos E2 - Gral. Santos 1170 c/ Concordia

Teléfono: (+595 21) 217 9000

Correo electrónico: comunicacion@mitic.gov.py

Mesa de entrada: sgeneral@mitic.gov.py

Asunción – Paraguay

Entorno personal de aprendizaje (PLE):
Curso de Ciberseguridad: Seguridad en medios digitales

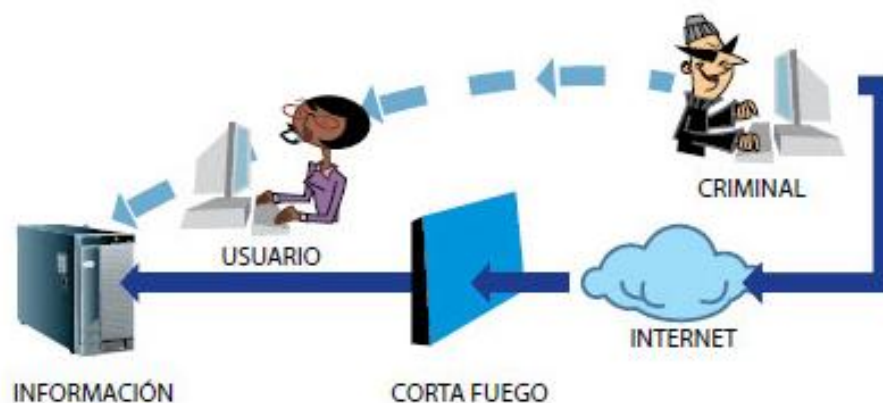
Todas las imágenes presentes en este material de apoyo educativo han sido reconocidas y, en todos los casos, son de uso libre. Todas las fuentes bibliográficas utilizadas en este material de apoyo educativo son citadas mediante el gestor de referencias bibliográficas Zotero, desarrollado por el Center for History and New Media de la Universidad George Mason, utilizando el estilo de la American Psychological Association Séptima Edición.

1. Concepto de Ingeniería Social

1.1. ¿Qué es la Ingeniería Social?

La ingeniería social es una técnica mediante el cual el atacante busca, a través de la interacción humana y haciendo uso de habilidades sociales, engañar a la víctima para obtener información personal o de una organización para acceder a sus sistemas informáticos. De ahí su nombre, "social", ya que explotan el aspecto social y psicológico del ser humano.

Los ataques de ingeniería social muchas veces buscan, a través del engaño, que el usuario realice una acción tal como ingresar a un enlace o abrir un archivo, que infectan el equipo del usuario y le proporcionan al atacante un punto de entrada para la siguiente fase del ataque.



Cuando un atacante externo desea obtener una información dada, por lo general, necesita saltarse varias capas de seguridad tecnológica: un cortafuegos, un sistema de detección y prevención de intrusos, antivirus, y otro tipo de herramientas tecnológicas. Muchas veces es más difícil y más costoso evadir controles tecnológicos, explotar vulnerabilidades de sistemas o equipos, que engañar a una persona. Por lo general, las personas de la organización tienen un acceso más "directo" a la información, ya que son usuarios legítimos. Muchas veces, la protección entre una persona legítima y la información es una simple contraseña.

Unidad 3. Ingeniería Social

Como atacante, ¿para qué necesitaría realizar un complejo ataque de contraseñas, invirtiendo en capacidad de cómputo importante, con el tiempo y conocimiento que eso requiere, bajo el riesgo de ser detectado o que mi ataque no tenga éxito, si puedo en cambio, simplemente, enviar un correo falso a la víctima de modo a que ésta me dé su contraseña? De eso se trata la ingeniería social: muchas veces, es más fácil engañar a un ser humano, un ser social con reacciones basadas en sentimientos, que a la tecnología.

La ingeniería social no tiene límites: depende únicamente de la creatividad del atacante. En algunos casos, los intentos de engaño serán poco sofisticados y será fácil darse cuenta que se trata de un intento de ingeniería social. Sin embargo, en otros casos, el atacante podrá realizar un engaño sumamente sofisticado y creíble. A lo largo de este módulo veremos algunos ejemplos de técnicas de ingeniería sociales más utilizadas.

2.Principios de la Ingeniería Social

2.1. Fundamentos

La ingeniería social se aprovecha de los sentimientos humanos, los cuales todas las personas tenemos y a los cuales, en mayor o menos medida, somos susceptibles: la curiosidad, la empatía, el miedo, la vergüenza.

El principio que sustenta la ingeniería social es el que en cualquier sistema "los usuarios son el eslabón débil".

Podemos citar 4 principios básicos en los que se apoya un atacante para llevar a cabo un ataque de ingeniería social:

1. "Todos queremos ayudar"
2. "El primer movimiento es siempre de confianza hacia el otro"
3. "No nos gusta decir No"
4. "A todos nos gusta que nos alaben"

Dato curioso: estos principios fueron formulados por Kevin Mitnick, un ingeniero social muy famoso, que estuvo entre los criminales más buscados de Estados Unidos y hoy en día es un consultor de seguridad.

3. Tipos de Ingeniería social

3.1. Categorías

Vamos a comentar algunas de las técnicas más comunes de ingeniería social, diferenciándolos en dos categorías principales: ataques locales, donde el ingeniero social, es decir, el atacante, tiene acceso físico a la persona u organización que pretende atacar, y ataques remotos, donde no hay interacción física entre ambos. Por supuesto, un ataque puede tener varias etapas e incluir más de una técnica de ingeniería social, de ambas categorías:

ATAQUES LOCALES

- **Impersonificación:** un atacante se puede hacer pasar físicamente por otra persona de confianza: un técnico de una empresa de soporte de confianza, un vendedor de un producto o solución que a la víctima le interesa, un cliente interesado en los servicios de la organización, o cualquier otra persona que pueda parecer de confianza. Si bien, hablamos de impersonificación física, también podría ser de forma virtual: por teléfono, por correo electrónico u otros.
- **Tailgaiting:** un atacante, aprovechándose de la solidaridad y buena voluntad de otros, trata de "colarse" a algún área de acceso restringido. Por ejemplo, un empleado (la víctima) está ingresando a la empresa, la cual posee algún tipo de restricción en su acceso físico, por ejemplo: tarjetas RFID, molinetes, etc. El atacante irá corriendo con una gran "sonrisa" detrás de la víctima haciendo un gesto de haber olvidado su tarjeta de acceso. En caso de existir un molinete, ingresará junto a la víctima, disculpándose por su "torpeza".
- **Falla en controles físicos de seguridad:** se aprovecha de los controles físicos. Por ejemplo, si en la entrada de una organización se cuenta con un guardia o recepcionista que debe restringir un determinado acceso, un atacante podría tratar de convencerlo para que lo dejara pasar, por ejemplo, alegando que debe reunirse con una persona de la empresa. Dependiendo de lo convincente que sea la excusa y lo entrenada que esté la víctima en cuanto a las políticas, el ataque podrá ser exitoso.

Unidad 3. Ingeniería Social

- **Dumpster Diving:** una técnica muy utilizada es revisar la basura, ya que muchísimas veces se arrojan papeles con información sensible sin haberlos destruidos previamente: usuarios y contraseñas que fueron anotadas en algún papel, números de cuentas, correos impresos, planillas con información personal de los empleados, etc. También se suelen encontrar distintos medios de almacenamiento sin su debida destrucción, como CDs, discos duros, etc.
- **Shoulder Surfing:** denominamos así a la técnica de espiar por encima del hombro de las personas. De esta manera se puede observar lo que está tecleando la víctima y así deducir su password, PIN o patrones de desbloques en teléfonos.
- **Pendrivel olvidado:** otra técnica popular es hacer llegar un pendrive con algún software malicioso (por ejemplo, un keylogger que captura todas las pulsaciones del teclado) a una o más personas de una organización.

ATAQUES REMOTOS

- **Phishing:** en el módulo anterior mencionamos un ejemplo a través de correos electrónicos. En general, esta técnica busca “pescar” víctimas, de modo a que éstas le revelen alguna información (contraseñas, PIN, u otro). El engaño puede ser a través de correo electrónico, redes sociales, u otro medio. Por lo general, se busca que la víctima ingrese a un enlace falso y proporcione sus credenciales, o infectarlo con algún software malicioso que sirva para robar información y/o obtener un acceso.
- **Telefónico:** los engaños pueden ser también a través de una llamada telefónica, donde el atacante se hace pasar por alguien de confianza para que la víctima le revele información o realice alguna acción que le sea de utilidad al atacante. Éste puede hacerse pasar por un encuestador, por un funcionario de un organismo de control, por un técnico de la empresa de servicio de Internet, incluso por un empleado de la empresa que está ausente, o cualquier otra variante que se le ocurra.
- **Watering Hole (pozo de agua):** primeramente, el atacante compromete un sitio web muy utilizado por un grupo específico de personas, por ejemplo, un foro muy popular sobre una herramienta que utilizan los diseñadores gráficos de una organización. Este sitio web infectado es el “pozo de agua”. Las víctimas, cuando accedan al sitio web comprometido, podrían quedar infectados con el software malicioso que el atacante colocó allí.

4. Redes sociales e información personal en Internet

4.1. Información personal

Uno de los factores más peligrosos, es la creciente tendencia por parte de los usuarios de compartir información personal y sensible en forma constante. Desde imágenes de toda su familia, los lugares que frecuentan, gustos personales, estados de ánimo y relaciones amorosas. Las redes sociales proveen de mucha información a un delincuente para que realice un ataque, como para robar tu identidad o en el menor de los casos ser convincente para tener empatía.

Si un atacante no conoce nada sobre su víctima, es poco probable que pueda engañarlo, ya que será poco convincente. Si en cambio, conoce cierta información sobre ella, podrá idear una excusa más personalizada, y la víctima tenderá a confiar en él, aun cuando la información que posea no sea precisamente "secreta". Muchas veces exponemos en Internet información que, de por sí sola, no es sensible, pero no somos conscientes que la hemos publicado. Luego, cuando un atacante utilizara esa información para hacernos creer que nos conoce o que es confiable, muchas veces cometemos el error de creer: "esta persona sabe esto de mí, lo que me dice debe ser cierto".



Unidad 3. Ingeniería Social

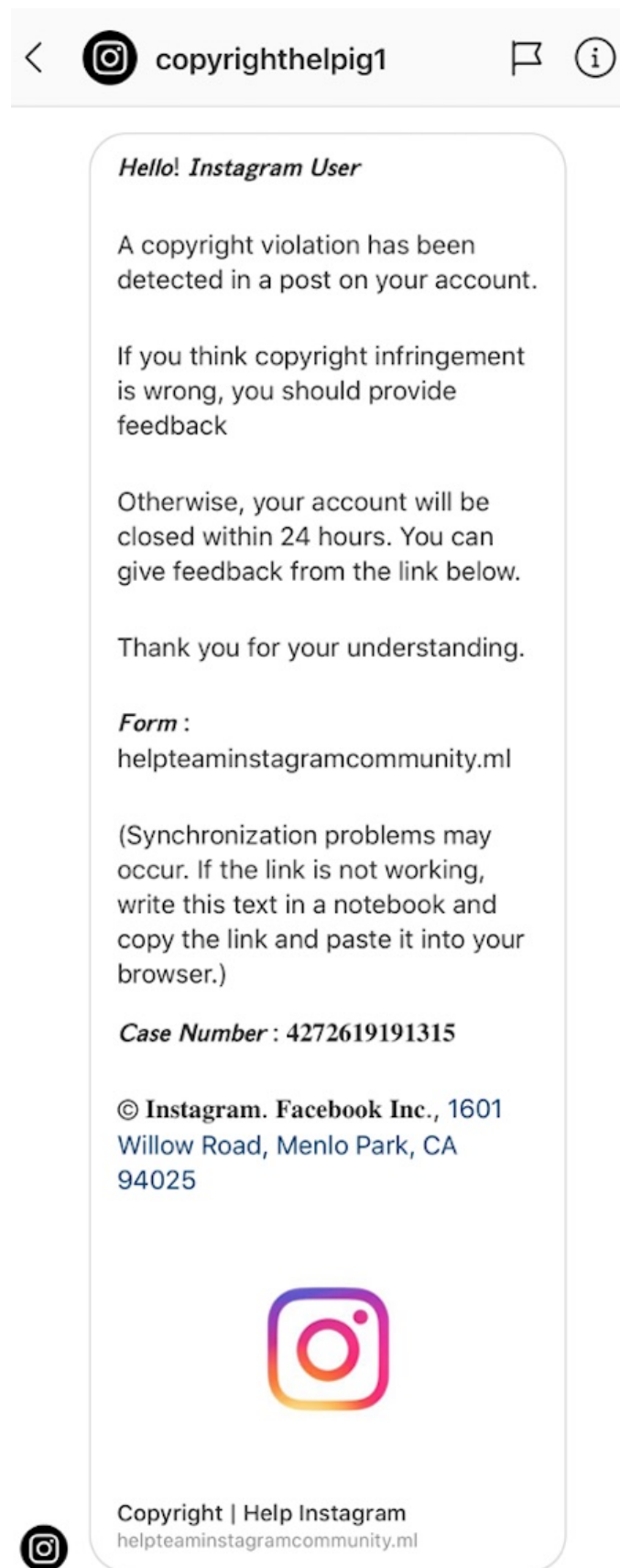
También tenemos que tener en cuenta que hoy en día, las redes sociales son un mecanismo más que un criminal puede utilizar para contactarnos. Por ejemplo, los mensajes de phishing, que anteriormente se distribuían únicamente mediante correo electrónico, hoy en día en cambio también nos pueden llegar a través de un mensaje directo de Facebook, Instagram, un mensaje de Whatsapp, etc.

5. Ejemplos de ingeniería social para el secuestro de cuentas

5.1. Ingeniería social en redes sociales

Hoy en día las redes sociales son, no solamente una plataforma de entretenimiento y conexión entre amigos y familiares, sino en muchos casos es incluso una herramienta de trabajo. Negocios, emprendimientos y profesionales de contenido utilizan las redes sociales como Facebook e Instagram tanto para mostrar sus productos o servicios, concretar ventas o incluso generar contenido digital. Esto hace que el valor de una cuenta de una red social trascienda el ámbito privado y tenga un valor incluso para el negocio. Es por ello que muchos criminales, conscientes de este valor, han puesto sus ojos en las cuentas de redes sociales; sobre todo, las cuentas con muchos seguidores tienen un alto valor.

En los últimos tiempos, muchas personas o empresas han sido víctimas de ciberdelincuentes que logran comprometer y “secuestrar” la cuenta de la víctima. En la gran mayoría de los casos, los criminales utilizan técnicas de ingeniería social. Por lo general, el delincuente envía un mensajes directos a las víctimas desde cuentas falsas de. Estos mensajes informan sobre algún tipo de problema con la cuenta y contienen un enlace a una página “oficial” de soporte de la plataforma. Se trata de una página falsa (phishing), en la que solicitan el usuario y la contraseña de la cuenta de la víctima con el fin de “solucionar” el problema. Sin embargo, como es una página falsa, controlada por el atacante, esas credenciales que la víctima introdujo, terminan en poder de ese atacante, permitiéndole acceder a la cuenta del usuario. Si bien, esto puede ocurrir en cualquier plataforma, es en Instagram donde últimamente se han multiplicado los casos.

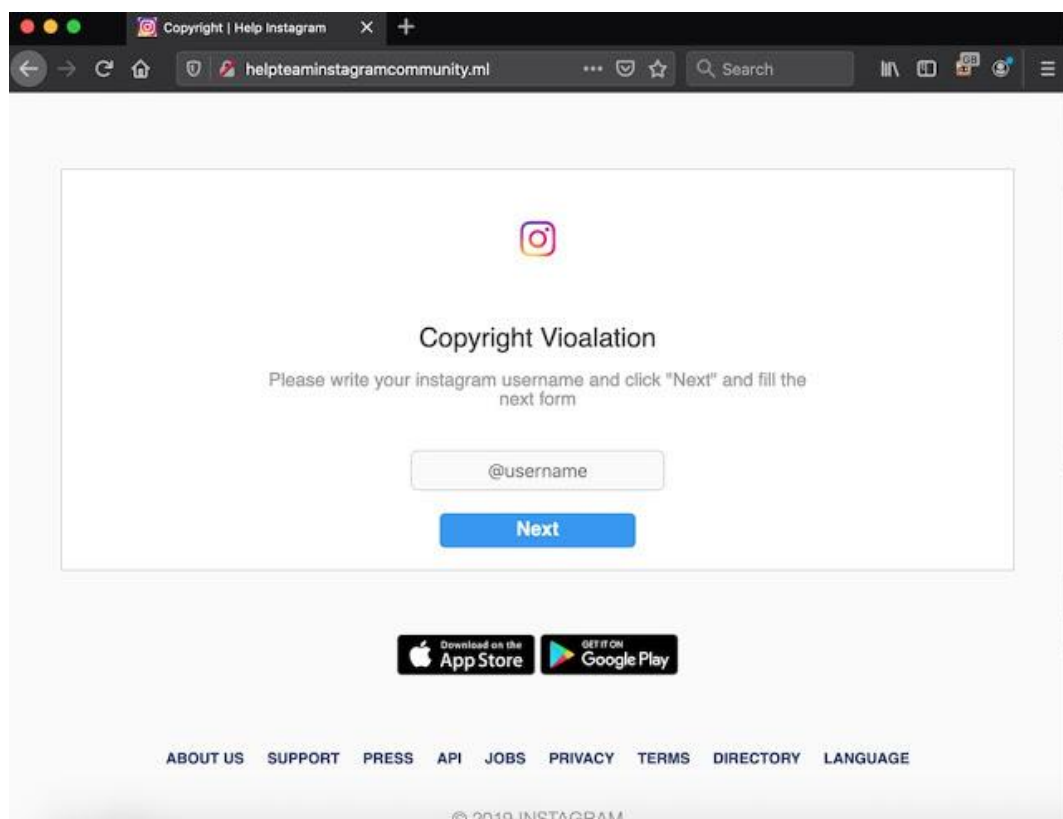


Unidad 3. Ingeniería Social

Uno de los ganchos más utilizados, trata de mensajes de infracción a los “derechos de autor” por parte del usuario, esta notificación es enviada a través de mensajes directos, desde una cuenta supuestamente “oficial” de Instagram, donde el ciberdelincuente incluye el logo de la compañía y un enlace a las políticas de copyright de Instagram en la descripción, con el objetivo de brindar una sensación de autenticidad. Muchas veces, la cuenta desde la cual el criminal envía este mensaje, es una cuenta que previamente se comprometió. Si el criminal logró comprometer una cuenta que estaba verificada y tenía muchos seguidores, eso incluso es más efectivo para engañar a las víctimas, que al ver que recibió un mensaje directo desde una cuenta verificada y con muchos seguidores, cree que se trata de una cuenta oficial real de Instagram.

Estos mensajes explican al usuario, sobre una supuesta infracción de la política de copyright en su cuenta y que es necesario ingresar al enlace adjunto antes de que pasen las 24 hs, caso contrario la cuenta será bloqueada.

El enlace, dirige a la víctima a una página de phishing aparentemente legítima, con el logo de Instagram y de apariencia similar al sitio web oficial. Por supuesto, es una página fasa. En esta página, se solicita primeramente el nombre de usuario.

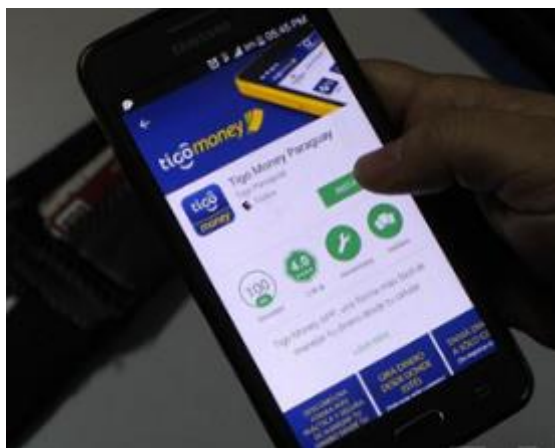


Unidad 3. Ingeniería Social

Una vez ingresado el nombre de usuario, la página procede a solicitar la contraseña de la cuenta, afirmando que, una vez el usuario ingrese la contraseña, su cuenta será suspendida mientras el “**problema**” sea resuelto. Finalmente, a modo de “**verificación**” solicitan las **credenciales de acceso** de la cuenta del **correo electrónico** asociada a Instagram, logrando así obtener acceso total a las cuentas tanto de correo electrónico como de Instagram.

5.2. Ingeniería social aplicada a billeteras electrónicas

También las billeteras electrónicas han sido blanco de criminales, quienes mediante engaños se hacen pasar por funcionarios de las compañías que ofrecen este tipo de servicios, con supuestas promociones y regalos para conseguir que la víctima caiga en el engaño y le revele los códigos de acceso a la misma, con lo que el criminal logra acceder a la billetera, realizar transferencias, etc. ¿Cómo funciona este ataque?



En primer lugar, el delincuente contacta a la víctima, por lo general, a través de una llamada telefónica. Se presenta generalmente como funcionario de la compañía que ofrece este tipo de servicios o alguien de confianza, como para generar confianza en la víctima, valiéndose de diversos métodos de ingeniería social. Por ejemplo, indica los datos personales de las víctimas como: nombre, cédula, fecha de nacimiento, hasta información del plan contratado, información crediticia, etc.

En algunos casos, previamente, el delincuente ya había obtenido datos personales de las víctimas. Los delincuentes consiguen estos datos de diversas fuentes, por ejemplo algunos datos son información pública, otras veces se extraen de redes sociales, o simplemente un tanteo de información obvia, o con alta probabilidad de ser acertadas; podría ser también

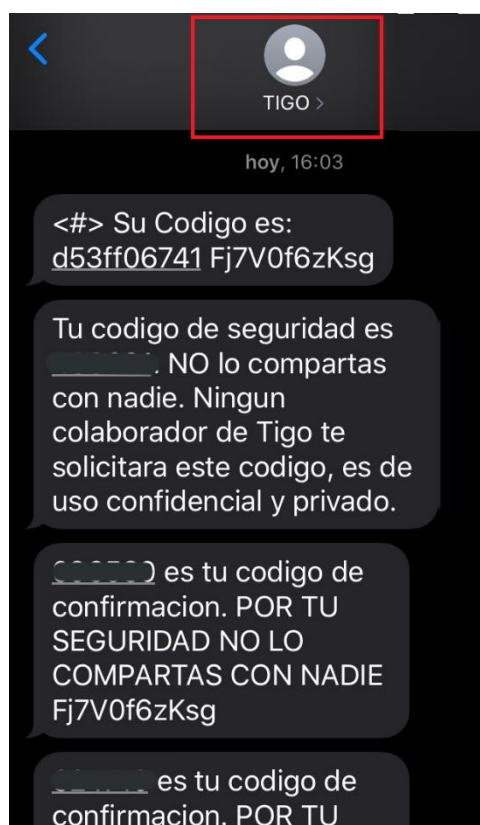
Unidad 3. Ingeniería Social

datos registrados en casas comerciales en las que las víctimas se han registrado en el pasado y que no han sido tratadas con el debido cuidado, es decir que han sido cedidas por una mala práctica de la misma o robada con o sin complicidad de la misma, o incluso tal vez de la propia compañía de los servicios de billetera, etc.

Además, el delincuente, previo al llamado a su víctima, prepara el escenario: descarga la aplicación de billetera electrónica de una de las compañías locales que ofrecen este servicio, desde las fuentes oficiales de descargas de aplicaciones, por ejemplo Google Play o App Store en teléfonos móviles.

Una vez descargada la aplicación, lo primero que ésta pide, es el número de teléfono a la que se va a asociar. Ahí es donde el delincuente ingresa el **número de teléfono de la víctima**. La aplicación realiza una comprobación del número ingresado, enviando un mensaje texto SMS al número introducido, es decir el número de la víctima.

Así, la víctima recibe un código de seguridad en ese mensaje de texto SMS enviado por la propia compañía que ofrece el servicio de billetera electrónica (porque es la aplicación la que a través de sus propios sistemas envía el mensaje).



Unidad 3. Ingeniería Social

A través de técnicas de ingeniería social el criminal busca ahora que la víctima le revele el código. La aplicación no puede funcionar sin el código de seguridad, por lo cual el delincuente lo necesita. Para ello es que contacta a la víctima para que, mediante engaños, éste revele el código de seguridad.

El delincuente logra ganarse la confianza de la víctima y finalmente lo convence que revele el código, a pesar de que en el SMS dice claramente que **NO LE REVELES A NADIE**, porque quien tenga ese código, luego puede acceder a tu billetera electrónica.

Muchas billeteras electrónicas incluso tienen dos códigos de seguridad, uno es el código aleatorio que genera la aplicación, y otro es una contraseña. Si, mediante engaños, la víctima revela también esa contraseña (o si esa contraseña es fácil de adivinar), el delincuente ya tiene acceso total a la billetera electrónica.

Durante la llamada, la excusa o gancho que el criminal puede utilizar, son diversos:

- Se presenta como funcionario de la telefónica y le dice que, como cliente fiel, ganó un premio de la telefónica y que le van a duplicar el saldo;
- Se presenta como funcionario del gobierno y le dice que accedió a algún subsidio
- Se presenta como funcionario de la empresa de Internet y le dice que debe verificar un problema con la conexión

Cualquier excusa es válida y depende de la creatividad del delincuente podrían usar relatos creíbles para ganarse la confianza y lograr que las víctimas caigan en el engaño.

Esta técnica no es exclusiva de billeteras electrónicas, puede aplicarse también a otras plataformas y aplicaciones como Whatsapp, redes sociales, cuentas bancarias, etc, ya que la mayoría de las aplicaciones que validan el número telefónico mediante un mensaje de texto SMS, envían un código de seguridad desde la propia aplicación o sistema, y si la víctima revela el código de seguridad, está permitiendo que el criminal "demuestre" a la aplicación que él es el dueño del número de teléfono. ¡Por eso, aunque recibas un código que sea de la aplicación misma, no le reveles a nadie!

Unidad 3. Ingeniería Social

5.2. Ingeniería social aplicada a aplicaciones de mensajería

Las aplicaciones de mensajería, especialmente Whatsapp, hoy en día son uno de los principales medios de comunicación en nuestro país, tanto para conversaciones familiares, entre amigos, en el ámbito profesional y empresarial, también son activos digitales que debemos proteger.

Son muy frecuentes los casos en los que los delincuentes utilizan ingeniosas técnicas para engañar a las potenciales víctimas, robar sus cuentas de WhatsApp, con diversos fines entre ellos robar dinero. Las víctimas son diversas, desde figuras públicas, personas mayores, jóvenes, profesionales, personas de nuestro círculo social, familiar, etc. Pero, cómo funciona realmente este método?

El método más común empieza cuando el delincuente instala WhatsApp en su teléfono, pero al momento de ingresar el número, en vez de ingresar su número, **ingresa el número de la víctima**. Para verificar el número, WhatsApp envía el código de verificación de 6 dígitos a ese número. Es decir, la víctima recibe un SMS (no solicitado) con un código. El criminal necesita ese código, no lo puede obtener sin engañar primero a la víctima.

Es ahí donde entra en juego las técnicas de "ingeniería social". La víctima es contactada por el delincuente (ya sea telefónicamente o por mensaje) y éste, bajo alguna excusa, le pide que le dicte o mande el código que recibió vía SMS. Las excusas pueden ser diversas:

El criminal puede comunicarse telefónicamente con la víctima y hacerse pasar por un personal de la telefónica o de un proveedor de Internet y que necesita el código para verificar algo del servicio

El criminal puede contactarse a través de Whatsapp y hacerse pasar por una persona de confianza, bajo la excusa de haber enviado erróneamente su código

Los temas de tendencia también son un posible gancho, como por ejemplo un supuesto agendamiento para la vacunación del COVID-19, la asignación de un subsidio del gobierno, etc.

Unidad 3. Ingeniería Social

A veces, el criminal ya robó previamente la cuenta de un contacto de confianza y nos escribe desde la cuenta robada, por lo que la víctima puede creer que su conocido le está pidiendo el código.



Una vez que el atacante logra convencer a la víctima y ya cuenta con el código que la víctima le proporcionó, lo ingresa en su teléfono y de esta manera logra "secuestrar" la cuenta de Whatsapp de la víctima. La víctima notará que pierde acceso a su cuenta de Whatsapp, ya que, como Whatsapp no permite dos sesiones móviles en simultáneo, como el criminal ya la abrió en su teléfono, la sesión se cierra en el teléfono de la víctima.

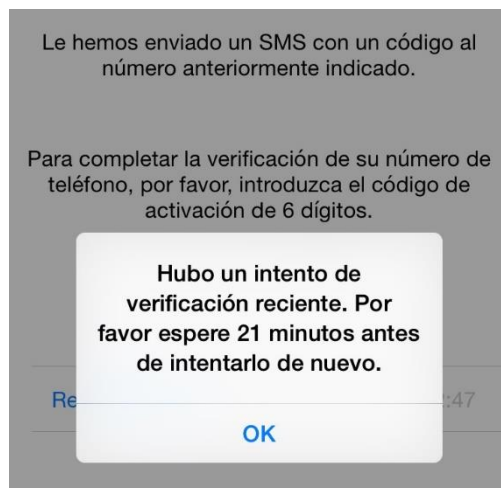
Si bien el criminal no puede leer las conversaciones pasadas, puede usar la cuenta para enviar mensajes haciéndose pasar por la víctima. En la mayoría de los casos que se vieron recientemente, lo usa para **solicitar dinero a los contactos** de la víctima haciéndose pasar por ella. En algunos casos, el criminal contacta a la víctima y la **extorsiona** para devolverle la cuenta.

En estos casos, es fundamental que la víctima, apenas se percate del secuestro de su cuenta, pueda reinstalar cuanto antes la aplicación y volver a realizar la verificación del número. De esta manera, se volverá a cerrar la sesión del criminal.

Se debe tener en cuenta que, últimamente, en muchos casos, cuando el delincuente logra acceder a la cuenta de WhatsApp, intencionalmente introduce el código de verificación de forma errada varias veces, tal que se bloquee temporalmente (por 7 horas) el envío de código de verificación, lo que le da 7 horas de acceso a la cuenta sin que el propietario real pueda recuperarla, pudiendo engañar durante más tiempo a los contactos de la víctima. Si al realizar el proceso de verificación, un mensaje te indica que debes esperar varias horas para

Unidad 3. Ingeniería Social

poder recibir otro código, se debe aguardar la cantidad de tiempo designada en el mensaje, no existe manera de acelerar ese proceso.



También está siendo frecuente que los delincuentes con acceso a la cuenta robada activen la verificación en dos pasos. En ese caso, se debe esperar siete días para poder verificar el número sin el código de verificación de dos pasos, o recurrir al centro de soporte de Whatsapp. La sesión del delincuente con tu cuenta, se cerrará en cuanto ingreses el código de verificación de seis dígitos enviado por mensaje SMS.

6. Cuidados frente a la ingeniería social

6.1. Recomendaciones

Muchas veces exponemos en Internet información que, de por sí sola, no es sensible, pero no somos conscientes que la hemos publicado. Luego, cuando un atacante utilizara esa información para hacernos creer que nos conoce o que es confiable, muchas veces cometemos el error de creer: "esta persona sabe esto de mí, lo que me dice debe ser cierto".

Por supuesto, esto muchas veces no es tan sencillo, ya que para alguien que está más capacitado, podrá parecerle obvio, para otra persona que no conoce de estos

Unidad 3. Ingeniería Social

riesgos, no lo será evidente. Por ello, la principal herramienta para prevenir la ingeniería social es la concienciación y capacitación permanente de los usuarios.

Algunas buenas prácticas que podemos mencionar, son las siguientes:

- Nunca reveles datos confidenciales como claves de acceso, números de tarjetas de crédito, cuentas bancarias, etc., ni por teléfono, ni por correo electrónico ni a una persona en la cual no tenga absoluta confianza.
- Nunca hagas clic en enlaces o adjuntos que te llegues a través de un e-mail u otro medio, si no está plenamente seguro de que es legítimo. Ante la duda, siempre consulta.
- Desconfía de cualquier mensaje en el que se le ofrece la posibilidad de ganar dinero con facilidad, ya sea a través de correo electrónico, redes sociales, mensajes o cualquier otro medio.
- Si es usuario de banca electrónica o de cualquier otro servicio que implique introducir en una web, datos de acceso, asegúrate de que la dirección de la web es correcta.
- No confíes en las direcciones de los remitentes de e-mail o en los identificadores del número llamante en el teléfono: pueden falsearse con suma facilidad.
- Limita la cantidad de información personal que publica en redes sociales o en Internet, en general. Siempre que publiques o compartas una información, ten en cuenta que ésta pasa a ser pública y que cualquiera la puede utilizar.
- **Utiliza el sentido común** y pregúntate siempre que recibas un mensaje o llamada sospechosa si alguien puede obtener algún beneficio de forma ilícita con la información que te están solicitando. Sé siempre desconfiado y precavido.
- Activa **autenticación de doble factor** (ver Módulo 1 "[Control de acceso - credenciales](#)"), pero recuerda que para que esta protección sea efectiva, **no debes compartir** el código A2F tampoco
- Siempre que recibas un mensaje o correo extraño o sospechoso de una persona conocida, trata de ponerte en contacto con la persona por algún otro medio (por ejemplo, una llamada).
- Si recibes un mensaje o llamada extraña de alguien que dice ser de una compañía de confianza (tu telefónica, tu banco, una institución de gobierno), contáctate personalmente con la compañía y consulta si el mensaje es real. Independientemente de la respuesta, recuerda no compartir datos como contraseñas, códigos, etc.